

## Detecting Malicious Circuits in IP-Core

NOTE: The Solicitations and topics listed on this site are copies from the various SBIR agency solicitations and are not necessarily the latest and most up-to-date. For this reason, you should use the agency link listed below which will take you directly to the appropriate agency server where you can read the official version of this solicitation and download the appropriate forms and rules.

The official link for this solicitation is: <http://www.acq.osd.mil/osbp/sbir/solicitations/index.shtml>

Agency:  
Department of Defense

Release Date:  
November 20, 2013  
Branch:  
Office of the Secretary of Defense

Open Date:  
November 20, 2013  
Program / Phase / Year:  
SBIR / Phase I / 2014

Application Due Date:  
January 22, 2014

Solicitation:  
[2014.1](#)

Close Date:  
January 22, 2014  
Topic Number:  
OSD14.1-IA2

### Description:

**OBJECTIVE:** Develop technologies and tools for detecting potential malicious/backdoor logics in hardware IP-core, toward reducing supply-chain vulnerability in embedded computing and system on chip environment. **DESCRIPTION:** This topic solicits the development of technologies and tools which perform analysis on gate-level netlist of hardware IP-core to identify potentially malicious wires and logics, related to hardware backdoors. Compromise at hardware level is very powerful, difficult to detect and generally not addressable via software running on it. The solicited tool can be used to screen, detect and disqualify components/IP-cores which contain backdoor circuitry. Tactical computing devices often rely on the system-on-chip embedded computing hardware commonly found in embedded computing devices, often used in mobile computing and networking appliances, as the underlying processing infrastructure. Modern large and complex embedded and system-on-chip (VLSI/FPGA circuit) design often integrates large number of pre-designed components, acquired from third parties. These IP-core components are generally delivered as gate-level netlist. Currently, there is no practical way to ensure that these third party components (IP-cores) do not contain any backdoor or malicious circuitry, which can stealthily compromise the design (system) after deployment. Compromise circuitry embedded within the hardware is generally very hard to detect and defeat. State of the art methodology for verifying VLSI design includes running unit test on the individual component, as well as performing comprehensive regression test on the full-chip (VLSI) design. However, these tests can only address functionality described in the specifications. They rarely uncover the stealthy, out-of-specification malicious logics, which can only be triggered (activated), by hidden, rare and very-specific occasions. A new approach is needed to uncover these elusive circuits. If successful, the tools developed in this SBIR can be used to screen these third party

IP-cores to ensure that they do not contain any backdoor/malicious logic. They prevent compromised IP-cores from being integrated into the design and enhance the security of the system. PHASE I: Investigate and develop creative methods, techniques for reliably discovering malicious/backdoor logics in hardware IP-core, normally delivered in the form of gate-level-netlist. Develop proof of concept prototype and identify the metrics that determine the prototype's efficacy. PHASE II: Develop and enhance the prototype into a fully functioning tool. Demonstrate and evaluate the capability of the tool on actual (real world scale) set of benign IP-Cores and IP-cores with malicious-circuit/ backdoor. PHASE III DUAL USE APPLICATIONS: Inclusion of third party IP-cores is a common practice in system-on-chip design and development in private sector and in military industry. These SOC's hardware have been the backbones for embedded and mobile computing devices in the commercial sector as well as in the military uses. System-on-chip (SOC) hardware (semiconductors) is widely used in commercial application such as network appliances and mobile computing. Security and financial motive for the insertion malicious circuits exists in these applications. Commercial chip provider/manufacturers have interest for ensuring that their product is free of malicious circuits. If successful the tool developed within this SBIR should find its market in the commercial sector as well as military sector.